Better value, delivered.

IG/POL001
Data Protection Policy

www.ypo.co.uk

Document Type	Policy	
Document Ownership	Head of Finance	
Title of Document	Data Protection Policy	
Status	Live	
Reference number	IG/POL001	
Controlled by	Executive Director - Finance	
Agreed with Unison / date:	N/A	
Approved by / date:	Simon Hill – Managing Director	S C Hill S C Hill (Aug 8, 2024 21:53 GMT+1)
Publication date	26 August 2024	
Next Review date	1 year	
Current Version	v.2	
Replaces document	Data Protection Policy 2015 (no reference)	
Connected Documents	IG/POL002 Data Subject Access Request Policy IG/POL003 Data Protection Impacts Assessment Policy IG/POL004 Records Retention and Disposal Policy IG/POL005 Data Subject Erasure Request Policy IG/POL006 Personal Data Breach Management Policy IG/OR001 Record of Processing Activity IG/RA001 Legitimate Interests Assessment	

IG/POL001 Data Protection Policy

1.0 Scope

1.1 This policy relates to:

All permanent, fixed term, and temporary employees, any third-party representatives or sub-contractors, interns and agents engaged with YPO in the UK or overseas; and

All Personal Data that is obtained, stored or otherwise processed by YPO, whether it is held in electronic or manual form.

2.0 Responsibilities

2.1 YPO have appointed a DPO to oversee compliance with Data Protection Law.

2.2 The DPO can be contacted by emailing dataprotection@ypo.co.uk

2.3 The DPO's responsibilities include:

- Monitor compliance with the UK General Data Protection Regulations and other data protection laws, and with YPO's data protection policies.
- Raising awareness of data protection within the organisation and supporting with staff training.
- Providing advice with regard to our Data Protection Impact Assessments and monitoring their performance.
- Cooperating with the UK's Supervisory Authority (currently the Information Commissioner's Office, also known as the ICO); and
- Acting as a contact point for Data Subjects and the Information Commissioner's Office.

3.0 Objectives

4.1 To help us meet the regulatory requirements of data protection legislation, we have developed a set of objectives.

4.2 YPO will:

- Develop, implement, and maintain policies and procedures governing the collection, processing and disposal of Personal Data to ensure they are in accordance with UK GDPR.

- Only obtain, store and process Personal Data when we have a valid, lawful basis for doing so.

- Monitor all organisation practices for compliance with UK GDPR.

- Record and maintain our processing activities as evidence of compliance with the accountability principle.

- Ensure that all employees are provided with training so that they are aware of their responsibilities and obligations with regards to our business.

- Be open and transparent with our Data Subjects so that they feel confident and secure when providing us with their Personal Data knowing that it will be processed in compliance with Data Protection Law.

- Continually review our practices and policies with regard to Data Protection Law to identify any non-compliance issues before they become a risk.

- Protect the rights of Data Subjects provided to them by Data Protection Law and ensure that we have suitable facilities in place to help Data Subjects exercise their rights.

- Utilise appropriate technical and organisational security measures to ensure the security of Personal Data processed.

- Ensure that Personal Data is not transferred outside of the UK to a country without an adequacy decision without appropriate safeguards in place for doing so.

4.0 Data Protection Legislation

4.1 YPO recognises that it is subject to the following legislation in the UK:

- The UK General Data Protection Regulations
- The Data Protection Act 2018
- The Data Protection (Charges and Information Regulations) 2018.
- Privacy and Electronic Communications Regulations 2003 (PECR).

5.0 The Information Commissioner's Office

5.1 The Information Commissioner's Office is an independent regulatory office whose role it is to uphold individuals' information rights.

5.2 Under the UK's Data Protection Laws, the ICO, as the UK's supervisory authority, can issue enforcement notices.

5.3 YPO is a Data Controller under data protection legislation, which means that it determines what purposes Personal Data will be used for and how it will be used. As a Data Controller, we are required to register with the ICO as a Data Controller and pay a fee.

5.4 Our ICO registration number is: **Z5734139.**

6.0 Data Protection Principles

6.1 YPO regards the lawful and correct treatment of Personal Data as very important to successful working, and to maintaining the confidence of those with whom we deal.

6.2 YPO intends to ensure that / Personal Data is treated lawfully and correctly.

6.3 To this end, YPO will adhere to the Principles of Data Protection, as detailed in the UK GDPR.

6.4 Specifically, the Principles require that Personal Data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with that purpose or those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form which permits identification of the Data Subject(s) for no longer than is necessary for the purposes for which the Personal Data is processed; and
- Processed in a manner that ensures appropriate security of the Personal Data.

6.5 YPO will also ensure that it can demonstrate its compliance with these principles at all times in accordance with the accountability principle in UK GDPR Article 5(2).

7.0 Lawful Processing Conditions

7.1 Article 6 of UK GDPR defines the lawful bases for Processing. Prior to carrying out any processing activity on Personal Data, YPO will always identify and establish the legal basis for Processing and verify this with the regulation. We will not process any Personal Data unless one of the following conditions are met:

- Consent - The Data Subject has given Consent to the Processing of his or her Personal Data for one or more specified purposes.
- Performance of a contract - Processing is necessary for the performance of a contract to which the Data Subject is party.
- Legal obligation - Processing is necessary for compliance with a legal obligation to which the Data Controller are subject.
- Vital interests - Processing is necessary in order to protect the vital interests (life or death situation) of the Data Subject or of another natural person.
- Public task – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Legitimate interests - Processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by a Third Party.

7.2 Our legal basis for Processing is documented and maintained on our Record of Processing Activities document (**IG/OR001**) which is maintained by the DPO.

8.0 Consent

8.1 Where any of our processing activities rely on the Data Subjects' consent, we will ensure that we collect their consent in accordance with UK GDPR. Under UK GDPR, consent must be:

- Freely given – The Data Subject must have a genuine choice, and where there is an imbalance of power between the Data Controller and the Data Subject, for example employer and employee, consent cannot be considered freely given.
- Specific – The Data Controller must explain its purpose(s) for the Processing of the Personal Data so that the Data Subject can Consent to the purpose(s) specifically.

- Informed – The Data Subject must be given all necessary details of the processing activity so that they can comprehend how the Processing might affect them.

- An unambiguous indication – The Data Subject's statement or clear affirmative action must leave no doubt as to their intention to give Consent; and

- A clear affirmative action – The Consent is given on an opt-in basis, for example an unticked box which the Data Subject can then tick themselves.

8.2 YPO will maintain auditable records of Data Subject consent for Processing Personal Data and will always be able to demonstrate that the Data Subject has consented to Processing of their Personal Data where applicable.

8.3 YPO also ensure that the Data Subject can withdraw their consent as easily as they managed to give it, and where their consent is withdrawn, we will respect their wishes.

8.4 YPO will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

9.0 Legitimate Interests

9.1 If we rely on legitimate interests as our lawful condition for Processing and collecting Personal Data, then we will be transparent with the Data Subject about what our legitimate interests are. These interests will be explained and justified clearly to the data subject.

9.2 We will take into consideration how the data subject may reasonably expect us to use their Personal Data, and we will cease to process their Personal Data where the rights of the Data Subject override our legitimate interests.

9.3 Where we are relying on our legitimate interests for Processing Personal Data, in some circumstances it may be necessary for the DPO to perform a Legitimate Interests Assessment (**IG/RA001**) to ensure that the interests of the organisation are fairly balanced with the rights and freedoms of individuals.

9.4 Where an LIA has been undertaken, a copy of this will be retained in order to demonstrate accountability.

10.0 Data Subject Rights

10.1 Data protection legislation affords numerous rights to Data Subjects concerning their Personal Data:

- The right to be informed – Data Subjects should be provided with information about how and why their Personal Data will be used.
- The right of access – Data Subjects can request access to copies of all of the Personal Data held by YPO about them. The process for handling a Data Subject Access Request is detailed in the Data Subject Access Request Policy (**IG/POL002**).
- The right to rectification – Data Subjects can request that YPO rectifies any incomplete or incorrect data which YPO holds about them.
- The right to erasure – Data Subjects can request that YPO erases their data, and we will comply as far as is necessary. The process for handling a Data Subject Erasure Request is detailed in the Data Subject Erasure Request Policy (**IG/POL005**).
- The right to restriction of Processing – Data Subjects can request that YPO stops Processing their Personal Data for particular purposes.
- The right to data portability – Data Subjects can request that YPO transfers their Personal Data directly to another Data Controller.
- The right to object to Processing – Data Subjects can object to YPO Processing their Personal Data in certain situations.

10.2 According to Article 22 of the UK GDPR, an individual also has 'the right not to be subject to a decision based solely on automated decision making, including Profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. No automated decision making, or Profiling takes place at YPO.

10.3 YPO will ensure that Data Subjects' rights are upheld at all times.

11.0 Privacy Notices

11.1 When collecting an individual's Personal Data, YPO will ensure that they have been provided with the required information according to Articles 13 and 14 of UK GDPR, known as 'fair processing information'.

11.2 YPO has taken every step to ensure that the information provided is:

- Concise.
- Transparent.
- Intelligible.
- Easily accessible; and
- Written using clear, plain language.

12.0 Data Storage

12.1 Information and records relating to Data Subjects will be stored securely and will only be accessible to authorised personnel.

12.2 In accordance with the storage limitation principle, information will be stored for only as long as is necessary and will be disposed of appropriately.

12.3 YPO have specified retention periods and disposal methods for all records which YPO processes in the Records Retention and Disposal Policy (**IG/POL004**).

12.4 For further guidance on data retention, see YPO's Records Retention and Disposal Policy.

12.5 It is YPO's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a Third Party.

13.0 Data Sharing

13.1 In order to carry out our daily functions, YPO may share Personal Data with third parties providing a service (Data Processors or other Data Controllers). In this event, YPO will ensure that there is an appropriate contract in place ensuring that the Personal Data shared is appropriately protected by the Third Party.

13.2 The Data Subject will be made aware, in most circumstances, of how and with whom their information will be shared through Privacy Notices.

13.3 Where necessary, YPO will obtain the Data Subject's consent before sharing their Personal Data.

14.0 Data Protection by Design

14.1 YPO is proud to operate a data protection by design approach to the protection of Personal Data and we consider the safety and security of the Personal Data that we hold in every processing activity we undertake, from the beginning through to completion.

14.2 This approach means that:

- We are able to identify any issues concerning our processing activities and take action before they become a risk.
- There is an increased awareness of data protection.
- We are able to demonstrate how we comply with data protection legislation in accordance with the accountability principle.
- Actions we take are less likely to have a negative impact on the privacy of Data Subjects.

14.3 Our data protection by design approach to protecting Personal Data ensures the security of data that is processed, particularly when it is shared and/or transferred. Where reasonably possible, appropriate technical and organisational measures are implemented as recommended by data protection legislation, including:

- Pseudonymisation – we refer to data using a pseudonym where technically and reasonably possible.
- Encryption – Hardware and software is encrypted where technically and reasonably possible.
- Data minimisation – only the data which is necessary for YPO's processing activities is collected.
- Restriction – access controls are in place for all Third Party systems which YPO uses which means only authorised individuals can access Personal Data.
- Data Protection Impact Assessments – before we begin any new processing activities, we will consult with our DPO and complete a DPIA where it is deemed necessary. The procedure for carrying out a DPIA is detailed in our Data Protection Impact Assessments Policy (**IG/POL003**).

15.0 Personal Data Breaches

15.1 A Personal Data breach is a breach of security leading to the accidental or unlawful:

- Destruction.
- Loss.
- Alteration; or
- Unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

15.2 A Personal Data breach that results in a risk to the rights and freedoms of Data Subjects must be reported to the ICO by the DPO within 72 hours of YPO becoming aware of the breach.

15.3 In some situations (where the breach results in a high risk to the rights and freedoms of individuals) the affected Data Subjects must also be notified.

15.4 Decisions on whether a Personal Data Breach leads to a report to the ICO or notified to the affected Data Subject must be retained.

15.5 For guidance on how to recognise a Personal Data breach and how to report one, see the Personal Data Breach Management Policy (**IG/POL006**).

16.0 Definitions

16.1 **Consent of the Data Subject** means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

16.2 **Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

16.3 **Data Processor** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

16.4 **Data Protection Impact Assessment** has the meaning given to it in IG/POL003.

16.5 **Data Protection Law** means the rules set out by the UK Government to determine how Personal Data can and should be used including the legislation set out at paragraph 4.0 of this Policy all interpretations thereof which are determined by the English Judiciary as part of a ruling regarding the same.

16.6 **Data Protection Officer or DPO** means an individual or organisation appointed by YPO to monitor its compliance with Data Protection Law.

16.7 **Data Subject** means the identified or identifiable living individual to whom Personal Data relates**.**

16.8 **Legitimate Interest Assessment or LIA** is a light touch risk assessment to ensure YPO is Processing information lawfully.

16.9 **Personal Data** means any information relating to an identified or identifiable natural person.

16.10 **Principles of Data Protection** have the meaning given to them by the UK GDPR.

16.11 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

16.12 **Profiling** means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

16.13 **Supervisory Authority** means an independent public authority which is established by the UK Government.

16.14 **Third Party** means a natural or legal person, public authority, agency or body other than the Data Subject or YPO.

16.15 **UK General Data Protection Regulations or UK GDPR** means the rules designed to protect the rights and freedoms of individuals through the regulation of what Personal Data can be collected, processed retained or otherwise used by YPO.